ПРИЛОЖЕНИЕ № 2

к Требованиям к созданию, развитию
и функционированию трансграничного
пространства доверия

ТРЕБОВАНИЯ
к средствам удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза

I. Общие положения

1. Настоящие Требования устанавливают требования к средствам удостоверяющего центра службы доверенной третьей стороны интегрированной информационной системы Евразийского экономического союза (далее соответственно – удостоверяющий центр, Союз).

II. Требования к программному обеспечению средств удостоверяющего центра

2. Программное обеспечение средств удостоверяющего центра не должно содержать средств, позволяющих модифицировать или искажать алгоритм работы программного обеспечения средств удостоверяющего центра.

3. Прикладное программное обеспечение средств удостоверяющего центра и программное обеспечение средств криптографической защиты информации, используемых удостоверяющим центром, должны использовать только документированные функции системного программного обеспечения.

4. Системное и прикладное программное обеспечение средств удостоверяющего центра должно обеспечивать разграничение доступа

системного администратора средств удостоверяющего центра, администратора сертификации средств удостоверяющего центра, операторов средств удостоверяющего центра и пользователей удостоверяющего центра к информации, обрабатываемой средствами удостоверяющего центра, в соответствии с правилами разграничения доступа, установленными системным администратором средств удостоверяющего центра.

5. В состав системного и (или) прикладного программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий очистку оперативной и внешней памяти, используемой для хранения информации ограниченного доступа.

6. Исходные тексты системного и прикладного программного обеспечения средств удостоверяющего центра должны пройти проверку реализации методов и способов защиты информации от атак, для подготовки и проведения которых используются возможности нарушителя безопасности информации, указанные в утверждаемой Евразийской экономической комиссией (далее – Комиссия) модели угроз безопасности информации и действий нарушителя в удостоверяющем центре службы доверенной третьей стороны.

7. В состав программного обеспечения средств удостоверяющего центра должен входить механизм, обеспечивающий устойчивость к компьютерным атакам из внешних сетей.

8. Исходные тексты системного и прикладного программного обеспечения средств удостоверяющего центра должны пройти формальную верификацию отсутствия недекларированных возможностей, а также формальную верификацию реализации методов

и способов защиты информации противостояния атакам, для подготовки и проведения которых используются возможности нарушителя безопасности информации, указанные в утверждаемой Комиссией модели угроз безопасности информации и действий нарушителя в удостоверяющем центре службы доверенной третьей стороны.

III. Требования к аппаратным средствам удостоверяющего центра

9. К аппаратным средствам удостоверяющего центра предъявляются следующие требования:

а) проведение проверки соответствия реализации целевых функций удостоверяющего центра с использованием определяемой Комиссией системы тестов аппаратных средств удостоверяющего центра;

б) проведение специальной проверки аппаратных средств удостоверяющего центра, произведенных в третьих странах, в целях выявления устройств, предназначенных для негласного получения информации;

в) проведение исследований аппаратных средств удостоверяющего центра и анализа программного кода BIOS с целью исключения наличия недекларированных возможностей, а также исследований на соответствие требованиям к защите от утечки информации по каналам побочных электромагнитных излучений и наводок, установленным в соответствии с законодательством государств – членов Союза (далее – государства-члены).

IV. Требования к ролевому разграничению

10. В средствах удостоверяющего центра должны реализовываться следующие обязательные роли:

а) системный администратор, в полномочия которого входят инсталляция, конфигурация и поддержка функционирования средств удостоверяющего центра, создание и поддержка профилей членов группы администраторов средств удостоверяющего центра, конфигурация профиля и параметров журнала аудита;

б) администратор сертификации, в полномочия которого входят создание и аннулирование сертификатов ключей проверки электронной цифровой подписи (электронной подписи) (далее – ЭЦП);

в) администратор аудита, в полномочия которого входят просмотр, копирование и полная очистка журнала аудита;

г) оператор, в полномочия которого входят резервное копирование и восстановление информации, хранимой в средствах удостоверяющего центра.

11. В средствах удостоверяющего центра должен реализовываться механизм, исключающий возможность авторизации одного члена группы администраторов средств удостоверяющего центра с целью использования полномочий различных ролей.

12. Системный администратор не должен иметь возможности вносить изменения в журнал аудита.

V. Требования к целостности средств удостоверяющего центра

13. В средствах удостоверяющего центра должен реализовываться механизм контроля несанкционированного случайного и (или)

преднамеренного искажения (изменения, модификации) и (или) разрушения информации, программных и (или) аппаратных средств удостоверяющего центра (далее – контроль целостности). Требования к механизму контроля целостности определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

14. Контроль целостности должен осуществляться при каждой перезагрузке операционной системы до ее загрузки, а также динамически в процессе функционирования средств удостоверяющего центра (динамический контроль целостности).

15. Динамический контроль целостности должен выполняться не реже 1 раза в сутки.

16. В составе программных и (или) аппаратных средств удостоверяющего центра должны иметься средства восстановления целостности программных средств удостоверяющего центра.

VI. Требования к управлению доступом

17. Средства удостоверяющего центра должны обеспечивать реализацию дискреционного и мандатного принципов управления доступом, а также создание замкнутой рабочей среды (программной среды, которая допускает существование в ней только фиксированного набора программ и процессов). Требования к управлению доступом определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

VII. Требования к идентификации и аутентификации

18. Идентификация и аутентификация включают в себя распознавание пользователя средств удостоверяющего центра, члена

группы администраторов средств удостоверяющего центра или процесса, а также проверку их подлинности. Механизм аутентификации при отрицательном результате аутентификации должен блокировать доступ этих субъектов доступа к функциям удостоверяющего центра.

19. В средствах удостоверяющего центра для любой реализованной процедуры аутентификации должен применяться механизм ограничения количества следующих подряд попыток аутентификации одного субъекта доступа, число которых не должно быть более 3. При превышении числа следующих подряд попыток аутентификации одного субъекта доступа доступ этого субъекта доступа к средствам удостоверяющего центра должен быть заблокирован на промежуток времени, который определяется в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

20. Описание процедуры регистрации пользователей средств удостоверяющего центра (внесения данных в реестр пользователей средств удостоверяющего центра), в том числе требование о необходимости предъявления пользователем средств удостоверяющего центра при регистрации документов, удостоверяющих личность, должны содержаться в эксплуатационной документации на средства удостоверяющего центра.

21. В отношении лиц, осуществляющих доступ к средствам удостоверяющего центра, должна проводиться двухфакторная аутентификация.

22. Для пользователей средств удостоверяющего центра и членов группы администраторов средств удостоверяющего центра допускается реализация механизмов удаленной аутентификации на основе

разрешенных криптографических алгоритмов с использованием сертификатов аутентификации.

23. При осуществлении локального доступа к средствам удостоверяющего центра аутентификация членов группы администраторов средств удостоверяющего центра должна выполняться до перехода в рабочее состояние таких средств (например, до загрузки базовой операционной системы).

24. При использовании для локальной аутентификации символьного, периодически изменяемого пароля он должен состоять из не менее 8 символов (при общем количестве символов алфавита не менее 36). Период изменения пароля не должен превышать 6 месяцев.

VIII. Требования к защите данных, полученных или передаваемых удостоверяющим центром

25. Самоподписанный сертификат ключа проверки ЭЦП удостоверяющего центра должен храниться способом, исключающим его модификацию или искажение.

26. Средства удостоверяющего центра должны обеспечивать передачу данных, содержащих информацию ограниченного доступа, полученных удостоверяющим центром или передаваемых из удостоверяющего центра, способом, исключающим несанкционированный доступ к информации.

27. Средства удостоверяющего центра должны реализовывать защиту от навязывания ложных сообщений (действий, воспринимаемых субъектами электронного взаимодействия или средствами удостоверяющего центра как передача истинного сообщения способом, защищенным от несанкционированного доступа) на основе

разрешенных криптографических алгоритмов с использованием сертификатов ключа проверки ЭЦП. Требования к процедуре защиты от навязывания ложных сообщений определяются в техническом задании на разработку (модернизацию) средств удостоверяющего центра.

28. Средства удостоверяющего центра должны реализовывать процедуру защищенной передачи пользователем средств удостоверяющего центра первоначального запроса на создание для него сертификата ключа проверки ЭЦП.

29. Средства удостоверяющего центра должны принимать критичную для функционирования удостоверяющего центра информацию в случае, если она подписана ЭЦП.

30. Все компоненты средств удостоверяющего центра должны размещаться в одной контролируемой зоне.

IX. Требования к регистрации событий

31. Операционная система средств удостоверяющего центра должна поддерживать ведение журнала аудита, содержащего информацию системных событий и событий, связанных с выполнением удостоверяющим центром своих функций.

32. Список регистрируемых в журнале аудита событий должен содержаться в эксплуатационной документации на средства удостоверяющего центра.

33. Журнал аудита должен быть доступен только администратору аудита.

34. Полная очистка журнала аудита проводится только после копирования всей информации, подлежащей очистке. После такой очистки в качестве первой записи в журнале аудита должен

автоматически регистрироваться факт проведения очистки (с указанием даты, времени проведения указанной очистки и информации о лице, которое ее проводило).

X. Требования к надежности и устойчивости функционирования средств удостоверяющего центра

35. Производится расчет вероятности возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим центром своих функций.

36. В течение суток вероятность возникновения сбоев и неисправностей аппаратных средств удостоверяющего центра, приводящих к невыполнению удостоверяющим центром своих функций, не должна превышать аналогичную вероятность возникновения сбоев и неисправностей используемых в составе удостоверяющего центра криптографических средств.

37. Средняя наработка средств удостоверяющего центра (комплексно) на отказ составляет не менее 18 000 ч.

38. Должно осуществляться тестирование устойчивости функционирования средств удостоверяющего центра.

39. Время восстановления средств удостоверяющего центра составляет не более 4 часов.

40. Меры и средства повышения надежности и устойчивости функционирования средств удостоверяющего центра должны предусматривать квотирование ресурсов средств удостоверяющего центра.

XI. Требования к созданию, использованию, хранению и уничтожению ключевой информации

41. Порядок создания, использования, хранения и уничтожения ключевой информации, а также сроки ее действия определяются в соответствии с требованиями, установленными в эксплуатационной документации на средства ЭЦП и иные криптографические средства, используемые средствами удостоверяющего центра.

42. Копирование ключевой информации должно осуществляться в соответствии с эксплуатационной документацией на используемые в удостоверяющем центре криптографические средства. Не допускается копирование информации ключевых документов (криптографических ключей, в том числе ключей ЭЦП) на носители (например, жесткий диск), не являющиеся специализированными ключевыми носителями, без ее предварительного шифрования, которое должно осуществляться с применением встроенной функции используемого средства криптографической защиты информации.

43. Ключ ЭЦП, используемый для подписания создаваемых средствами удостоверяющего центра сертификатов ключей проверки ЭЦП и подписания сообщений службы доверенного времени и службы подтверждения статусов сертификатов, должен генерироваться, храниться, использоваться и уничтожаться в отдельных криптографических модулях (доверенных вычислительных устройствах).

44. Ключ ЭЦП, используемый для подписания создаваемых сертификатов ключей проверки ЭЦП и подписания списка уникальных номеров сертификатов ключей проверки ЭЦП, действие которых в определенный момент времени до истечения срока их действия было

прекращено удостоверяющим центром (далее – список отозванных сертификатов), не должен использоваться в иных целях.

XI. Требования к резервному копированию информации и восстановлению работоспособности средств удостоверяющего центра

45. Средства удостоверяющего центра должны реализовывать функции резервного копирования информации, обрабатываемой средствами удостоверяющего центра, и восстановления работоспособности аппаратных средств удостоверяющего центра в случае повреждения такой информации и таких средств. В ходе резервного копирования должна быть исключена возможность копирования криптографических ключей.

46. Данные, сохраненные при резервном копировании, должны быть достаточными для восстановления функционирования средств удостоверяющего центра до состояния, зафиксированного на момент копирования данных.

47. Должны быть приняты меры по обнаружению несанкционированных изменений сохраненных данных.

48. Требования к времени восстановления работоспособности средств удостоверяющего центра должны быть определены в техническом задании на разработку (модернизацию) средств удостоверяющего центра, а также в эксплуатационной документации на средства удостоверяющего центра.

49. Сохраняемая при резервном копировании защищаемая информация должна сохраняться только в зашифрованном виде.

XIII. Требования к созданию и аннулированию сертификатов ключей проверки ЭЦП

50. Протоколы создания и аннулирования сертификатов ключей проверки ЭЦП должны быть описаны в эксплуатационной документации на средства удостоверяющего центра.

51. Создаваемые удостоверяющим центром сертификаты ключей проверки ЭЦП и списки отозванных сертификатов должны соответствовать требованиям, установленным приложением № 4 к Требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 2017 г. № .

52. Средства удостоверяющего центра должны реализовывать механизм контроля соответствия создаваемых сертификатов ключей проверки ЭЦП требованиям, установленным приложением № 4 к Требованиям к созданию, развитию и функционированию трансграничного пространства доверия, утвержденным Решением Совета Евразийской экономической комиссии от 2017 г. № .

53. Средства удостоверяющего центра должны реализовывать аннулирование сертификата ключа проверки ЭЦП с использованием списков отозванных сертификатов и протокола OCSP.

54. Средства удостоверяющего центра в отношении владельца сертификата ключа проверки ЭЦП должны реализовывать проверку уникальности ключа проверки ЭЦП и проверку обладания соответствующим ключом ЭЦП.

XIV. Требования к реестру выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП и к предоставлению доступа к нему

55. В средствах удостоверяющего центра должны быть реализованы механизмы хранения и поиска по атрибутам выданных удостоверяющим центром, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП в реестре выданных, прекративших действие и аннулированных сертификатов ключей проверки ЭЦП (далее – реестр сертификатов), а также механизмы предоставления сетевого доступа к реестру сертификатов.

56. Все вносимые в реестр сертификатов ключей проверки ЭЦП изменения должны регистрироваться в журнале аудита.

XV. Требования к криптографическим средствам

57. Средства удостоверяющего центра должны использовать средства ЭЦП и иные криптографические средства, имеющие заключение уполномоченных органов государства пребывания Комиссии о соответствии требованиям, установленным законодательством этого государства к криптографическим средствам класса КА, а также соответствующие принципам разработки и модернизации шифровальных (криптографических) средств защиты информации, утверждаемым Комиссией.

58. Для создания и проверки ЭЦП средства удостоверяющего центра должны использовать средства ЭЦП, реализуемые на основе криптографического модуля, имеющего в своем составе средства отображения результатов создания (проверки) ЭЦП.

XVI. Требования к криптографическим стандартам

59. Средства удостоверяющего центра должны использовать средства ЭЦП и иные криптографические средства, реализующие криптографические алгоритмы, идентификаторы которых указаны в приложении № 8 к Положению об обмене электронными документами при трансграничном взаимодействии органов государственной власти государств – членов Евразийского экономического союза между собой и с Евразийской экономической комиссией, утвержденному Решением Коллегии Евразийской экономической комиссии от 28 сентября 2015 г. № 125.

XVII. Требования к проверке действительности сертификата ключа проверки ЭЦП

60. Реализованный в средствах удостоверяющего центра механизм проверки ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП должен быть указан в эксплуатационной документации на средства удостоверяющего центра. Такой механизм должен обеспечивать проверку ЭЦП в выдаваемых удостоверяющим центром сертификатах ключей проверки ЭЦП после создания сертификата ключа проверки ЭЦП и до его выдачи.

61. При проверке действительности сертификата ключа проверки ЭЦП средства удостоверяющего центра проверяют действительность каждого сертификата из цепочки сертификатов ключей проверки ЭЦП, в том числе действительность ЭЦП, которыми подписаны такие сертификаты. Данная цепочка состоит из корневого самоподписанного сертификата ключа проверки ЭЦП удостоверяющего центра и проверяемого сертификата ключа проверки ЭЦП.

XVIII. Дополнительные требования

62. В целях ограничения возможностей построения атак на средства удостоверяющего центра с использованием каналов связи должны применяться средства межсетевого экранирования, применяемые серверами, обслуживающими сайты, веб-службы и веб-приложения. Средства межсетевого экранирования должны обеспечивать контроль и фильтрацию информационных потоков по протоколу передачи гипертекста, проходящих к веб-серверу и от веб-сервера.

63. Должны применяться средства защиты от компьютерных вирусов, обеспечивающие обнаружение компьютерных программ или иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования защищаемой информации или нейтрализации средств защиты информации, а также обеспечиваться реагирование на обнаружение таких программ и информации.

64. Должны применяться средства защиты от компьютерных атак, обеспечивающие обнаружение действий, направленных на получение несанкционированного доступа к информации, оказание специальных воздействий на средства удостоверяющего центра в целях получения, уничтожения, искажения защищаемой информации и (или) блокирования доступа к ней, а также обеспечиваться реагирование на такие действия (предотвращение таких действий).

65. Средства межсетевого экранирования, средства защиты от компьютерных вирусов и средства защиты от компьютерных атак должны соответствовать требованиям, определяемым уполномоченными органами государств-членов.

66. Исследования средств удостоверяющего центра с целью подтверждения их соответствия настоящим Требованиям должны проводиться с использованием определяемых уполномоченными органами государств-членов числовых значений параметров и характеристик реализуемых в средствах удостоверяющего центра механизмов защиты информации.

67. Средства удостоверяющего центра должны эксплуатироваться в соответствии с эксплуатационной документацией на них. Организационно-технические мероприятия, необходимые для обеспечения безопасного функционирования средств удостоверяющего центра, должны указываться в эксплуатационной документации на средства удостоверяющего центра.